(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－98461

(43)公開日　平成11年(1999)４月９日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｎ	5/92		Ｈ０４Ｎ	5/92	Ｈ
Ｇ０６Ｆ	12/14	３１０	Ｇ０６Ｆ	12/14	３１０Ｚ
Ｇ０９Ｃ	5/00		Ｇ０９Ｃ	5/00	
Ｈ０４Ｎ	1/40		Ｈ０４Ｎ	1/44	
	1/44			1/40	Ｚ

審査請求　未請求　請求項の数９　ＯＬ　（全７頁）　最終頁に続く

(21)出願番号　特願平9－251185

(22)出願日　平成９年(1997)９月16日

(71)出願人　000002059
神鋼電機株式会社
東京都江東区東陽七丁目２番14号

(72)発明者　杉山　早実
三重県伊勢市竹ヶ鼻町100番地　神鋼電機株式会社伊勢事業所内

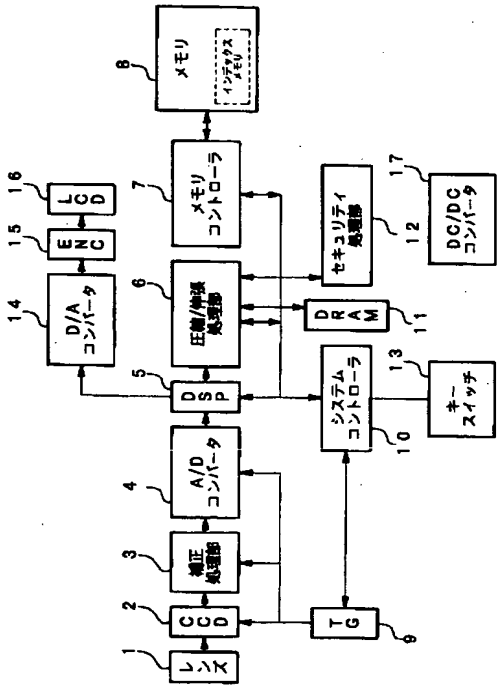
(74)代理人　弁理士　志賀　正武　(外11名)

(54)【発明の名称】　デジタル画像記録装置

(57)【要約】

【課題】　改ざんが行われたインデックス画像のチェックができるデジタル画像記録装置と、さらに画像そのものにセキュリティをかけ改ざん不能にすることができるデジタル画像記録装置の提供。

【解決手段】　画像データ２１をサンプリングしたインデックス画像データに対して電子印鑑と同様の原理により、一方向関数の逆関数を使って復号鍵データによりセキュリティをかけ、画像データを暗号化し、このセキュリティをかけられた画像データは、一方向関数を使って、予め与えられている公開鍵２５データを用いることにより暗号化インデックスデータ２４を復元し、原インデックスデータとの比較により改ざんの有無をチェックすることができる。さらに、画像データそのものに同様のセキュリティをかけ暗号化圧縮画像データとし、改ざん不能にする。



1

【特許請求の範囲】
【請求項１】　デジタル画像記録装置が取り込んだ画像データをデータ処理して記憶する記憶手段と、該記憶手段の記憶データを記録する記録媒体と、該記録媒体からデータを読み出し、このデータの編集を行うためのパソコンと、前記編集後の画像データを印刷するプリンタまたは前記画像データをデジタルデータとして記録、保存する保存媒体とからなる画像処理システムにおいて、
前記デジタル画像記録装置が取り込んだ画像データをサンプリングしてインデックス画像データを作成し、該インデックス画像データに対し電子印鑑と同様の原理により復号鍵による一方向関数の逆関数を用いて暗号化することを特徴とするデジタル画像記録装置。
【請求項２】　前記記録、保存されるデータは下記５種類のデータがセットデータとして記録、保存されることを特徴とする請求項１に記載のデジタル画像記録装置。
（１）圧縮された画像データ
（２）画像に対応した個別情報データ
（３）復号鍵によって暗号化されたインデックス画像データ
（４）暗号化されたインデックス画像データを復元するための公開鍵
（５）圧縮画像データからインデックス画像データを作成する作成方法
【請求項３】　前記画像データ改ざんの有無を判定するために、
前記公開鍵による一方向関数を使って前記暗号化されたインデックス画像を復元することを特徴とする請求項１または２に記載のデジタル画像記録装置。
【請求項４】　前記画像データ改ざんの有無の判定するために、
前記画像データからインデックス画像を作成し、この画像と前記公開鍵による一方向関数を使ってインデックス画像データを復元することを特徴とする請求項１または２に記載のデジタル画像記録装置。
【請求項５】　デジタル画像記録装置が取り込んだ画像データをデータ処理して記憶する記憶手段と、該記憶手段の記憶データを記録する記録媒体と、該記録媒体からデータを読み出し、このデータの編集を行うためのパソコンと、前記編集後の画像データを印刷するプリンタまたは前記画像データをデジタルデータとして記録、保存する保存媒体とからなる画像処理システムにおいて、
前記デジタル画像記録装置が取り込んだ画像データに対し、電子印鑑と同様の原理により復号鍵による一方向関数の逆関数を用いて暗号化することを特徴とするデジタル画像記録装置。
【請求項６】　前記記録、保存されるデータは下記３種類のデータがセットデータとして記録、保存されることを特徴とする請求項５に記載のデジタル画像記録装置。
（１）暗号化された圧縮画像データ

2

（２）画像に対応した個別情報データ
（３）暗号化された圧縮画像データを復元するための公開鍵
【請求項７】　前記復号鍵のデータは読み出し不可能な不揮発メモリ等に記録されることを特徴とする請求項１ないし６のいずれかに記載のデジタル画像記録装置。
【請求項８】　前記復号鍵のデータは個々のデジタル画像記録装置に固有のデータであることを特徴とする請求項７に記載のデジタル画像記録装置。
【請求項９】　前記復号鍵のデータは複数台のデジタル画像記録装置に共通のデータであることを特徴とする請求項７に記載のデジタル画像記録装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、デジタル画像記録装置の画像処理のうち、特に画像セキュリティシステムに関する。
【０００２】
【従来の技術】従来、工事写真等、証拠を証明する目的で使用される写真は、専ら銀塩写真が用いられてきた。しかし、ＣＣＤイメージセンサを用いたデジタルカメラの普及につれて、業務効率改善の一環としてこのデジタルカメラが採用されるようになりつつある。
【０００３】デジタルカメラを使った写真システムを図３に示す。この写真システムの概略は、まず、デジタルカメラ３１で目的の写真を撮影すると、この画像は、ＣＣＤイメージセンサに取り込まれ、相関二重サンプリング、ガンマ補正、自動ホワイトバランスの各補正処理が行われた後、このアナログ信号はデジタル値に変換処理される。さらに、デジタル信号プロセッサ（ＤＳＰ）によって各ピクセルに対応したＲ，Ｇ，Ｂデータに変換され、画像データの圧縮が行われた後、メモリに保存される。このメモリには画像データの他、撮影条件、日付、画像ファイル記号などの付随情報が記録される。
【０００４】次に、パソコン３７に画像を転送する方法には二通りの手段があり、その第１は、メモリカード３４など何らかのメモリにデータを保存し、パソコン３７に読み込む方法であり、第２の方法は、デジタルカメラ３１本体のインターフェース３３とパソコン３７のインターフェース３６とを接続し、データを伝送する方法である。さらに、パソコン３７にインストールされているアルバム編集用ソフト４１によって、工事アルバムに編集する。編集結果はプリンタ３９によりプリント出力し、アルバムとしてバインドされる。また、この編集結果はＣＤＲ４０によってＣＤ－ＲＯＭに仕上げられ、デジタルデータとして記録、保存される。
【０００５】
【発明が解決しようとする課題】ところが上述の方法ではデータ転送、画像編集の段階で画像を改ざんしようと思えば、容易に改ざんすることができ、証拠写真として

の信頼性に欠けるという問題点の解決が課題となっていた。本発明はこのような背景の下になされたもので、改ざんが行われた画像のチェックができるデジタル画像記録装置の画像セキュリティシステムと、さらに画像そのものにセキュリティをかけ改ざん不能にすることができるデジタル画像記録装置の画像セキュリティシステムとを提供することを目的とする。

【０００６】

【課題を解決するための手段】請求項１に記載の発明は、デジタル画像記録装置が取り込んだ画像データをデータ処理して記憶する記憶手段と、該記憶手段の記憶データを記録する記録媒体と、該記録媒体からデータを読み出し、このデータの編集を行うためのパソコンと、前記編集後の画像データを印刷するプリンタまたは前記画像データをデジタルデータとして記録、保存する保存媒体とからなる画像処理システムにおいて、前記デジタル画像記録装置が取り込んだ画像データをサンプリングしてインデックス画像データを作成し、該インデックス画像データに対し電子印鑑と同様の原理により復号鍵による一方向関数の逆関数を用いて暗号化することを特徴とするデジタル画像記録装置を提供する。

【０００７】請求項２に記載の発明は、前記記録、保存されるデータが下記５種類のデータがセットデータとして記録、保存されることを特徴とする請求項１に記載のデジタル画像記録装置を提供する。

（１）圧縮された画像データ

（２）画像に対応した個別情報データ

（３）復号鍵によって暗号化されたインデックス画像データ

（４）暗号化されたインデックス画像データを復元するための公開鍵

（５）圧縮画像データからインデックス画像データを作成する作成方法

【０００８】請求項３に記載の発明は、前記画像データ改ざんの有無を判定するために、前記公開鍵による一方向関数を使って前記暗号化されたインデックス画像を復元することを特徴とする請求項１または２に記載のデジタル画像記録装置を提供する。

【０００９】請求項４に記載の発明は、前記画像データ改ざんの有無の判定するために、前記画像データからインデックス画像を作成し、この画像と前記公開鍵による一方向関数を使ってインデックス画像データを復元することを特徴とする請求項１または２に記載のデジタル画像記録装置を提供する。

【００１０】請求項５に記載の発明は、デジタル画像記録装置が取り込んだ画像データをデータ処理して記憶する記憶手段と、該記憶手段の記憶データを記録する記録媒体と、該記録媒体からデータを読み出し、このデータの編集を行うためのパソコンと、前記編集後の画像データを印刷するプリンタまたは前記画像データをデジタル

データとして記録、保存する保存媒体とからなる画像処理システムにおいて、前記デジタル画像記録装置が取り込んだ画像データに対し、電子印鑑と同様の原理により復号鍵による一方向関数の逆関数を用いて暗号化することを特徴とするデジタル画像記録装置を提供する。

【００１１】請求項６に記載の発明は、前記記録、保存されるデータが下記３種類のデータがセットデータとして記録、保存されることを特徴とする請求項５に記載のデジタル画像記録装置を提供する。

（１）暗号化された圧縮画像データ

（２）画像に対応した個別情報データ

（３）暗号化された圧縮画像データを復元するための公開鍵

【００１２】請求項７に記載の発明は、前記復号鍵のデータが読み出し不可能な不揮発メモリ等に記録されることを特徴とする請求項１ないし６のいずれかに記載のデジタル画像記録装置を提供する。

【００１３】請求項８に記載の発明は、前記復号鍵のデータが個々のデジタル画像記録装置に固有のデータであることを特徴とする請求項７に記載のデジタル画像記録装置を提供する。

【００１４】請求項９に記載の発明は、前記復号鍵のデータが複数台のデジタル画像記録装置に共通のデータであることを特徴とする請求項７に記載のデジタル画像記録装置を提供する。

【００１５】

【発明の実施の形態】以下、この発明の一実施形態について図を参照しながら説明する。なお、デジタルカメラを使った写真システムの構成は「従来の技術」の項で説明した図３と同一である。図１はこの発明の一実施形態による画像セキュリティシステムを備えたデジタルカメラの構成を示すブロック図であり、図２は画像セキュリティシステムによる電子ファイル構造のイメージ図である。

【００１６】図１において、符号１はデジタルカメラ３１のレンズ、符号２はＣＣＤイメージセンサ、符号３は相関二重サンプリング（ＣＤＳ）、ガンマ補正（γ）、自動ホワイトバランス（ＡＷＢ）処理を行う補正処理部、符号４はアナログ信号をデジタル値に変換するＡ／Ｄコンバータ、符号５はデータを各ピクセルに対応したＲ，Ｇ，Ｂデータに変換するデジタル信号プロセッサ（ＤＳＰ）である。

【００１７】符号６は画像データの圧縮／伸張処理部であり、メモリ８に格納する場合は例えば、ＪＰＥＧ方式などによりデータの圧縮を行い、メモリ８からデータを読み出しＬＣＤモニタ１６に表示する場合はデータの伸張を行う。符号７はメモリコントローラであり、画像データのメモリへの書き込みまたは読み出しを行う。符号８は画像データ以外に、この画像データとセットになる撮影条件、日付、画像ファイル記号などの付随情報が記

録されるメモリである。符号９はＣＣＤセンサからデータを取り出すためのタイミングパルス生成部（ＴＧ）、符号１０はデジタルカメラ３１のシステム全体の制御を行うシステムコントローラ、符号１１はＤＲＡＭであり、画像データ処理を行うとき、このデータを一時的に保存するためのメモリである。

【００１８】符号１２はセキュリティ処理部であり、前記圧縮／伸張処理部６と連携してデータの改ざん防止処理を行う。符号１３はキースイッチであり、デジタルカメラ３１を立ちあげるための電源スイッチである。符号１４はＤ／Ａコンバータであり、画像データに基づきＬＣＤをアクティブ化する。符号１５は写真画像を表示する液晶表示器（ＬＣＤ）１６の表示器コントローラ（ＥＮＣ）である。

【００１９】次に、図１および図３によるデジタルカメラを使った写真システムのシステム図を参照して、この発明の一実施形態の動作を説明する。デジタルカメラ３１で目的の写真を撮影し、このデジタルカメラ３１のレンズ１を通して撮影された画像は、ＣＣＤイメージセンサ２に取り込まれ、補正処理部３において相関二重サンプリング、ガンマ補正、自動ホワイトバランスの各補正処理が行われた後、Ａ／Ｄコンバータ４においてデジタル値に変換され、さらに、デジタル信号プロセッサ（ＤＳＰ）５によって各ピクセルに対応したＲ，Ｇ，Ｂデータに変換される。

【００２０】工事写真では撮影されたデータが撮影後に改ざんされては証拠写真としての信頼性に欠けるので改ざん防止の対策を講じるが、この改ざん防止の方式には２種類の方式がある。まず第１の方式は画像データが改ざんされた場合、改ざんされたことをチェックできる方式であり、この方式について以下に説明する。上述のＤＳＰ５によって各ピクセルに対応したＲ，Ｇ，Ｂデータに変換された信号は、圧縮／伸張処理部６において圧縮されたデータをさらに間引き、インデックス画像データを作成する。この場合単純な間引きより、原画像を大きな圧縮率で圧縮し、インデックス画像とする方が望ましい。

【００２１】また、保存画像とこれに対応するインデックスとには１対１に対応するファイル記号がつけられ、常に一体のものとして扱われる。つまり、圧縮／伸張処理部６は画像データの圧縮、伸張の他、インデックス作成機能も合わせ持つ。メモリコントローラ７は、圧縮した画像およびインデックス画像データのメモリ８への書き込みと、このメモリ８からのデータの読み出しをコントロールする。

【００２２】セキュリティ処理部１２は前記インデックス画像に対して、電子印鑑と同様の原理により、一方向関数の逆関数を使って復号２５鍵データによりセキュリティをかけて画像データを暗号化し、暗号化インデックスデータとする。このセキュリティをかけられた暗号化

インデックスデータは、一方向関数を使って、予め与えられている公開鍵データを用いることにより暗号化インデックスデータとして復元することができ、原インデックス画像データとの比較により、データ改ざんの有無を判定することができる。

【００２３】上述の画像セキュリティシステムを備えたデジタルカメラから出力されるデータは次の５種類となり、図２（ａ）に示すように、電子記録メディアの電子ファイル２０に、リレーショナルな画像データセット２１として、次のようにセットで記録される。

（１）圧縮画像データ２２

（２）画像に対応した個別情報データ２３

（３）復号化キーでセキュリティのかけられた暗号化インデックスデータ２４

（４）セキュリティのかけられたインデックス画像データを復元するための公開鍵２５

（５）圧縮画像データからインデックスデータを作成するインデックス画像作成方法２６

【００２４】また、前記セキュリティ処理部１２の設定キーの中身は、数値あるいは計算式などのソフト的内容である。この設定キーが書き込まれるのは専用ＩＣであり、書き込みデータの設定はハード的に固定され、外部からこの書き込みデータを知ることは不可能である。もし、無理に調べようとすれば、ＩＣそのものが破損し、使用不可能になるようにすることもできる。また、セキュリティの設定は、基本的には個々のカメラに固有の値を設定するが、固有の値でなく共通の値とすることもできる。

【００２５】また、図２の画像ファイル２０に書き込まれる情報のうち、公開鍵２５、インデックス画像作成方法２６は必ずしも画像電子ファイル２０中に同時に書き込まれる必要はなく、例えばファイルの名称を一括に書き込んだインデックスファイル中に書き込むといった別の手段によって書き込んでも良い。

【００２６】これまでに説明してきたように、デジタルカメラからは画像データとセキュリティのかけられたインデックス画像が出力され、画像データはパソコンに取り込み画像の編集や画像の改ざんなどが自由に行えるが、セキュリティのかけられたインデックス画像は改ざんによりデータが破壊されてしまうので、改ざんは事実上不可能である。従って、写真画像が改ざんされたかどうかは、提出された写真画像と公開鍵を用いて復元したインデックス画像とを目視比較することによって改ざんされているかどうかをチェックすることができる。

【００２７】また、人間の目に頼らなくても画像データから、インデックスを作成したときと同一の処理を行ってインデックス画像データを作成し、この作成したインデックス画像データと公開鍵を用いて復元したインデックス画像データとが一致するかどうかをパソコンなどを使って検証することが可能となる。

【００２８】次に、データ改ざん防止の第２の方式について、上述の第１の方式と異なる部分について説明する。図１において、圧縮／伸張処理部６においてインデックスを作成せず、圧縮により作成された画像データそのものに復号鍵によって、セキュリティをかけ、メモリ７に格納する方式である。

【００２９】この方式では、上述の画像セキュリティシステムを備えたデジタルカメラから出力されるデータは次の３種類となり、図２（ｂ）に示すように、電子記録メディアの電子ファイル２０に、リレーショナルな画像データセット２１として、次のようにセットで記録される。

（１）暗号化して圧縮された暗号化圧縮画像データ２７

（２）画像に対応した個別情報データ２３

（３）セキュリティのかけられた暗号化圧縮画像データを復元するための公開鍵２５

この方式は、画像データそのものを暗号化するため信頼度が高いが、上述の第１の方式に比べ、暗号化と復号化に要する演算処理時間が長くなる。

【００３０】以上、本発明の一実施形態の動作を図面を参照して詳述してきたが、本発明はこの実施形態に限られるものではなく、本発明の要旨を逸脱しない範囲の設計変更等があっても本発明に含まれる。例えば、工事写真に限定せず、スキャナ、ビデオなどデジタル画像を扱い、かつセキュリティが問題となる全てのケースに適用できる。

【００３１】

【発明の効果】これまでに説明したように、この発明の一実施形態の第１の方式によれば、画像データをサンプリングしたインデックス画像データに対して電子印鑑と同様の原理により、一方向関数の逆関数を使って復号鍵データによりセキュリティをかけ、画像データを暗号化し、このセキュリティをかけられた画像データは、一方向関数を使って、予め与えられている公開鍵データを用いることにより暗号化インデックスデータを復元するようにしたので、改ざんが行われた画像のチェックを行うことができるという効果が得られる。

【００３２】さらに、この発明の一実施形態の第２の方式によれば、画像データそのものにセキュリティをかけ改ざん不能にすることができるという効果が得られる。

【図面の簡単な説明】

【図１】　この発明の一実施形態による画像セキュリティシステムを備えたデジタルカメラの構成を示すブロック図である。

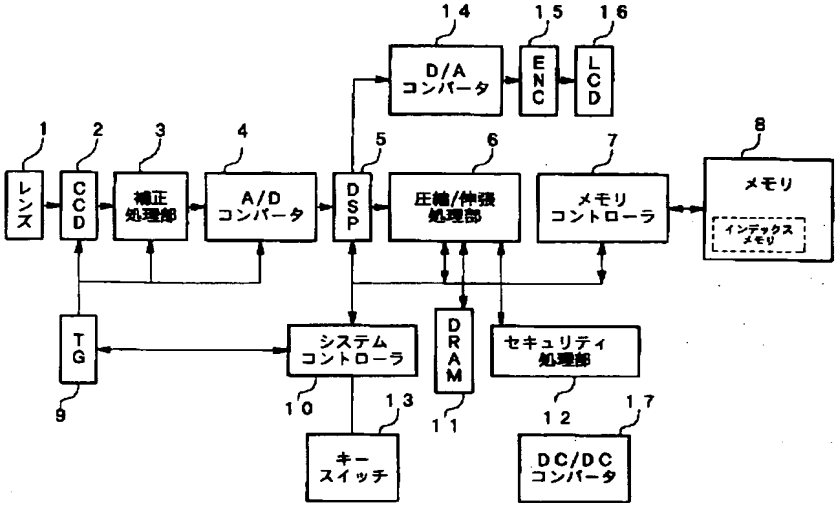
【図２】　画像セキュリティシステムによる電子ファイル構造のイメージ図である。

【図３】　デジタルカメラを使った写真システムを示す図である。

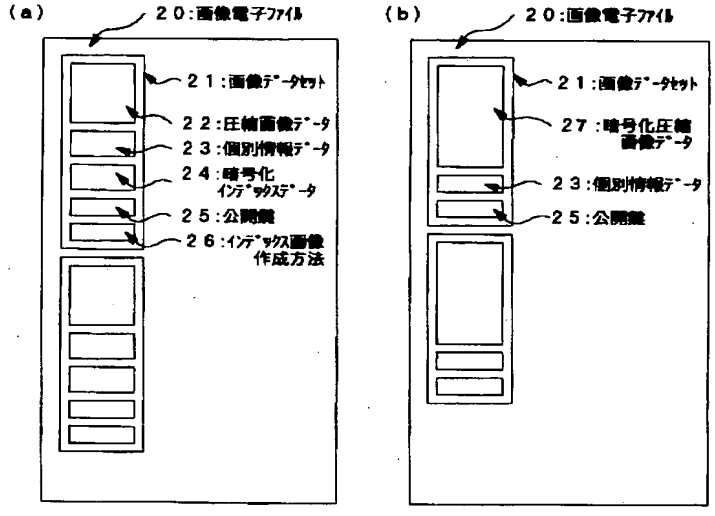
【符号の説明】

１　レンズ
２　ＣＣＤイメージセンサ（ＣＣＤ）
３　補正処理部
４　Ａ／Ｄコンバータ
５　デジタル信号プロセッサ（ＤＳＰ）
６　圧縮／伸張処理部
７　メモリコントローラ
８　メモリ
９　タイミングパルス生成部（ＴＧ）
１０　システムコントローラ
１１　ＤＲＡＭ
１２　セキュリティ処理部
１３　キースイッチ
１４　Ｄ／Ａコンバータ
１５　表示器コントローラ（ＥＮＣ）
１６　液晶表示器（ＬＣＤ）
１７　ＤＣ／ＤＣコンバータ
２０　画像電子ファイル
２１　画像データセット
２２　圧縮画像データ
２３　個別情報データ
２４　暗号化インデックスデータ
２５　公開鍵
２６　インデックス画像作成方法
２７　暗号化圧縮画像データ
３１　デジタルカメラ
３２　メモリカード挿入口
３３　インターフェース
３４　メモリカード
３５　ＰＣカードリーダ
３６　インターフェース
３７　パソコン
３８　ディスプレイ
３９　カラープリンタ
４０　ＣＤＲ
４１　アルバム編集ソフト

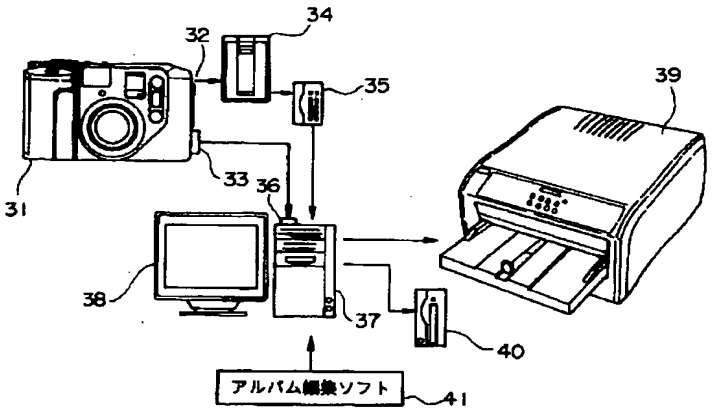
【図１】


1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
レンズ
CCD
補正処理部
A/Dコンバータ
DSP
圧縮/伸張処理部
メモリコントローラ
メモリ
インデックスメモリ
D/Aコンバータ
ENC
LCD
TG
システムコントローラ
DRAM
セキュリティ処理部
キースイッチ
DC/DCコンバータ

【図２】


(a)
２０:画像電子ファイル
２１:画像データセット
２２:圧縮画像データ
２３:個別情報データ
２４:暗号化インデックスデータ
２５:公開鍵
２６:インデックス画像作成方法
(b)
２０:画像電子ファイル
２１:画像データセット
２７:暗号化圧縮画像データ
２３:個別情報データ
２５:公開鍵

【図３】



フロントページの続き

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｎ　5/91		Ｈ０４Ｎ　5/91	Ｎ

Japanese Publication number : 11-98461 A

CLAIMS

[Claim(s)]
[Claim 1] The image pick-up section for being the digital of-evidence camera system which detects the alteration of the image data which picturized the photographic subject with the camera and was obtained, and picturizing a photographic subject, The cipher-processing section which creates the data for alteration detection from the image data obtained by the image pick-up using the encryption key built in beforehand, the camera to provide and the alteration detection section which detects whether said data for alteration detection were decrypted using the decryption key corresponding to said encryption key, and said image data was altered based on the result of this decryption -- since -- the digital of-evidence camera system characterized by becoming.
[Claim 2] The image pick-up section for being the digital of-evidence camera system which detects the alteration of the image data which picturized the photographic subject with the camera and was obtained, and picturizing a photographic subject, The cipher-processing section which creates the data for alteration detection from the image data obtained by the image pick-up using the encryption key built in beforehand, The camera to provide and the alteration detection section which detects whether said data for alteration detection were decrypted using the decryption key corresponding to said encryption key, and said image data was altered based on the result of this decryption, since -- the alteration supervision mode as which, as for said camera, said image data detects whether it was altered or not -- in addition, with the secure mode in which encryption to the image data transmitted to said alteration detection section from said camera is performed It has the digital-watermarking mode which embeds digital-watermarking data at image data, and the normal mode which performs the usual photography without using a security function. The digital of-evidence camera system characterized by having the mode selection section for choosing the mode of at least one request from these modes.
[Claim 3] The decryption key storage section memorized in accordance with the 1st decryption key corresponding to the 1st encryption key generated by equipment corresponding to the identifier of a proper, and this identifier, The decryption key output section which creates the data for alteration detection about said 1st decryption key using the 2nd encryption key, and is outputted in accordance with this data for alteration detection, and said 1st decryption key, A preparation ********** server and the decryption key storage section which memorizes said 1st decryption key acquired from said decryption

key server through means of communications etc., Said data for alteration detection supplied from said decryption key server through means of communications etc. are decrypted using the 2nd decryption key corresponding to said 2nd encryption key. the decryption key acquisition section equipped with the alteration detection section which detects whether said 1st decryption key was altered based on the result of this decryption -- since -- decryption key acquisition / registration system characterized by becoming.
[Claim 4] With the filing Management Department which is the digital image edit system into which image data is edited, and does filing management of the image data inputted through the image input section while detecting the alteration of image data While decrypting the 1st data for alteration detection beforehand given to said image data using the decryption key corresponding to the encryption key used when creating this data for alteration detection The alteration detection section which detects the alteration condition of image data by comparing this the 1st decoded data for alteration detection and said image data, To said image data from the edited image data to which various image processings were performed by the image editorial department which performs various kinds of image processings, and said image editorial department, and the data of the edit hysteresis by said image editorial department the renewal section of an image file which creates the 2nd data for alteration detection using an encryption key other than said encryption key, and adds this to said edited image data -- since -- the digital image edit system characterized by becoming.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to a digital of-evidence camera system, decryption key acquisition / registration system, and a digital image edit system.
[0002]
[Description of the Prior Art] The photograph analogically recorded on the film and media of the former, for example, a camera, and voice are used as what has the certification force in a trial etc. By advance of digital technique in recent years, the equipment which records an image and voice as digital data has spread. According to such digitization, the advantage which does not deteriorate even if it copies and which can be quickly distributed using a communication line in which processing and edit of the contents of information can be performed further easily is acquired. However, I hear that that processing and edit are easy can alter the contents of information easily by one side, there is, and room to suspect weight of the evidence as information is produced. Therefore, in order to enable it to use a digital image and voice as a piece of evidence, it is required to have the function to prevent the alteration of digital data by a certain approach. The camera which has such a prevention function is called the digital camera of evidence.
[0003] In order to realize this digital camera of evidence, it considers applying the

electronic signature technique generally used by the communication link etc. Two keys used as a pair are used in an electronic signature system. One is called a private key with the key for encryption, and another side is called a public key with the key for a decryption. It is enciphered using a private key and digital data is decrypted using a public key. Although a tropism function is used on the other hand in quest of a public key from a private key, on the other hand, this thing [asking for a private key] is mathematical very difficult from the public key conversely with the property of a tropism function. While it needs to be severely managed so that no men other than an owner can use a private key by any means, generally a public key is exhibited so that anyone can use.

[0004] The approach of alteration detection is a transmitting side and creates the code first called a message digest (Message Digest, following, MD) using a Hash Function etc. from the target digital data. If the method of extracting MD from the target digital data is exhibited and there are original data, anyone can extract MD. Incidentally, MD has the property in which a value changes a lot, when the original digital data differ from the good and known property.

[0005] Next, extracted MD is enciphered using a private key and he is a message authentication child (Message Authentication Code, following, MAC) about this. It carries out and transmits to the other party with original data. Here, the public key used as a private key and a pair shall be certainly passed to the addressee (an addressee may cross to the 3rd person's hand that what is necessary is just to surely have obtained the key).

[0006] In order to investigate that original data are not altered, first, a Hash Function etc. is used for a receiving side from original data, and it asks for MD'. Next, MAC is decrypted using a public key, MD is calculated, and it investigates whether this MD and MD' are in agreement. Even if original data are altered by the 3rd person, since the 3rd person does not have a private key, he cannot create MAC which can be decrypted with a public key, but becomes a different value from MD and MD'. This shows that original data were altered by the 3rd person.

[0007]

[Problem(s) to be Solved by the Invention] As described above, in order to detect the alteration of digital data, an electronic signature technique is applicable. However, when the approach of alteration detection which was described above was adopted as a digital camera of evidence, although it did not reveal by any means, conventionally, it was not easy to manage this private key on high security level, therefore, as for the private key as an encryption key, it was not able to heighten the weight of the evidence of a digital image.

[0008] Moreover, in the case of an image, there is the need of processing a data compression, field logging, insertion of a caption, etc. on the property of data, in many cases, but conventionally, by the approach of the electronic signature applied to document data, if it changes even when the contents of data are slight, it will be considered that data were altered. Therefore, in the conventional electronic signature system, required edit was not completed at all on the property of the above image data.

[0009] The place which this invention is made paying attention to such a technical problem,

and is made into the purpose The digital of-evidence camera system which can heighten the weight of the evidence of a digital image, and can manage an encryption key on very high security level, Decryption key acquisition - It is offering a registration system, and even if it edits compression which is further needed on the property of an image, field logging, insertion of a caption, etc., it is in offering the digital image edit system which can maintain the weight of the evidence of a digital image.

[0010]

[Means for Solving the Problem] In order to attain the above-mentioned purpose, the 1st invention The image pick-up section for being the digital of-evidence camera system which detects the alteration of the image data which picturized the photographic subject with the camera and was obtained, and picturizing a photographic subject, The cipher-processing section which creates the data for alteration detection from the image data obtained by the image pick-up using the encryption key built in beforehand, Said data for alteration detection are decrypted using the camera to provide and the decryption key corresponding to said encryption key, and it consists of the alteration detection section which detects whether said image data was altered based on the result of this decryption.

[0011] Moreover, the image pick-up section for the 2nd invention being a digital of-evidence camera system which detects the alteration of the image data which picturized the photographic subject with the camera and was obtained, and picturizing a photographic subject, The cipher-processing section which creates the data for alteration detection from the image data obtained by the image pick-up using the encryption key built in beforehand, Said data for alteration detection are decrypted using the camera to provide and the decryption key corresponding to said encryption key. It consists of the alteration detection section which detects whether said image data was altered based on the result of this decryption. Said camera Whether said image data was altered to the alteration supervision mode to detect In addition, the secure mode in which encryption to the image data transmitted to said alteration detection section from said camera is performed, It has the digital-watermarking mode which embeds digital-watermarking data at image data, and the normal mode which performs the usual photography without using a security function, and has the mode selection section for choosing the mode of at least one request from these modes.

[0012] The 3rd invention is decryption key acquisition / registration system. To equipment Moreover, the identifier of a proper, The decryption key storage section memorized in accordance with the 1st decryption key corresponding to the 1st encryption key generated corresponding to this identifier, The decryption key output section which creates the data for alteration detection about said 1st decryption key using the 2nd encryption key, and is outputted in accordance with this data for alteration detection, and said 1st decryption key, A preparation ********** server and the decryption key storage section which memorizes said 1st decryption key acquired from said decryption key server through means of communications etc., Said data for alteration detection supplied from said decryption key server through means of communications etc. are decrypted using the 2nd decryption key

corresponding to said 2nd encryption key. It consists of the decryption key acquisition section equipped with the alteration detection section which detects whether said 1st decryption key was altered based on the result of this decryption.

[0013] With moreover, the filing Management Department which the 4th invention is a digital image edit system into which image data is edited while detecting the alteration of image data, and does filing management of the image data inputted through the image input section While decrypting the 1st data for alteration detection beforehand given to said image data using the decryption key corresponding to the encryption key used when creating this data for alteration detection The alteration detection section which detects the alteration condition of image data by comparing this the 1st decoded data for alteration detection and said image data, To said image data from the edited image data to which various image processings were performed by the image editorial department which performs various kinds of image processings, and said image editorial department, and the data of the edit hysteresis by said image editorial department The 2nd data for alteration detection is created using an encryption key other than said encryption key, and it consists of the renewal section of an image file which adds this to said edited image data.

[0014]

[Embodiment of the Invention] Hereafter, the operation gestalt of this invention is explained to a detail with reference to a drawing. Drawing 1 is drawing showing the digital of-evidence camera structure of a system concerning the 1st operation gestalt of this invention, and consists of a digital camera 100 of evidence and alteration test equipment 101. The camera section 50-1 of the digital camera 100 of evidence has the image pick-up means 60 which consists of a taking lens 1, an image sensor 2, amplifier 3, A/D converter 4, and the signal-processing section 5. The photographic subject image which carried out incidence through the taking lens 1 is picturized by the image sensor 2. The electrical signal acquired by this image pick-up is amplified by the amplifier 3, and after being changed into a digital signal in the A/D-conversion section 4 and performing signal processing predetermined in the signal-processing section 5, it is memorized as image data in an image memory 6. The image data memorized in this image memory 6 is displayed on the image display section 7 if needed.

[0015] The image data memorized in the image memory 6 is changed into the graphics format of criteria, such as JPEG and TIFF, in the file-format-conversion section 8. Thereby, the file format by which the data of header information were added to image data is created ((A) of drawing 2). Next, in MD creation section 9, MD is created by applying predetermined functions, such as a Hash Function, to the data of the whole also including image data or a header ((B) of drawing 2). Next, in the MAC creation section 11, MAC is created by enciphering MD using the private key Kprivate (camera) memorized beforehand in the private key memory 10 ((C) of drawing 2). Next, at the header Records Department 11, created MAC is stored in an image header ((D) of drawing 2). At the filing Management Department 13, file management to the image file of the file format created by doing in this way is performed.

[0016] Such an image file demounts by control of the storage control section 15, and in order to detect whether it was altered while having been transmitted through the communication line 16 by control of the communications control section 14 while being memorized and carried by the possible storage 17 or, alteration detection equipment 101 is used.

[0017] That is, the image file memorized by the storage 17 with which alteration test equipment 101 was equipped is read to the filing Management Department 19 by control of the storage control section 18. Or the image file concerned is sent to the filing Management Department 19 through a communication line 25 by control of the communications control section 24. At the filing Management Department 19, an image file is divided into MAC and image data (header information other than the image data itself, such as JPEG and TIFF, may be included in this image data), MAC is inputted into the decryption section 21, and image data is inputted into MD creation section 22.

[0018] In the decryption section 21, MD1 is generated by decrypting MAC using the public key Kpublic (camera) memorized beforehand in the public key memory 20. This public key Kpublic (camera) and the above mentioned private key Kprivate (camera) are keys which serve as a pair in encryption/decryption processing. On the other hand, in MD creation section 22, MD2 is generated using predetermined functions, such as a Hash Function, from the inputted image data. Next, in the comparison coincidence section 23, when MD1 is compared with MD2 and both are not in agreement, it can judge with the image file having been altered by the 3rd person.

[0019] According to the above-mentioned 1st operation gestalt, the data (MAC) for alteration detection are created using the encryption key in a camera from image data, and it can check whether image data is altered by writing in this data for alteration detection in an image file, for example, the header information of an image. The weight of the evidence of the digital image it was presupposed that it was inferior of a digital image by this compared with the image conventionally photoed using the film can be heightened.

[0020] Moreover, by this operation gestalt, although the encryption key for creating the data for alteration detection is not revealed outside by any means including a camera user, since the encryption key for creating the data for alteration detection is beforehand stored in the memory area in a camera, it can manage an encryption key on very [in hard] high security level.

[0021] Next, the digital camera of evidence which has various kinds of modes (multimode) as the 2nd operation gestalt of this invention is explained. Here, the function of the request according to the purpose of using a camera can be set up by equipping a camera with the optional feature in the following various modes. Various modes are secure modes which encipher an image file here, the usual photography mode in which a security function is not used, the alteration supervision mode which gives alteration detection data to the photoed image file and the digital-watermarking mode which records the photoed copyright information on a photograph on an image file as digital watermarking, when saving an image file further at a dismountable storage, or when transmitting an image file

using communication facility.

[0022] Hereafter, with reference to drawing 3 , it explains to a detail further. What has the same reference number as drawing 1 in drawing 3 shall have the same function. In the digital camera 102 of evidence which consists of the camera section 50-2 in this operation gestalt, a user can choose [from] the desired mode among various kinds of modes described above in the mode selection section 31.

[0023] For example, when normal mode is chosen, the image data which picturized the photographic subject with the image pick-up means 60, and was obtained is memorized in an image memory 6. Especially in this mode, security mode does not work, but format conversion is carried out in the file-format-conversion section 8, the image data read from the image memory 6 is sent to the filing Management Department 13, and file management is carried out.

[0024] Moreover, when digital-watermarking mode is chosen, after image data is inputted into the digital-watermarking creation section 30 from the file-format-conversion section 8 and digital-watermarking data are embedded at the image data concerned, it is again returned to the file-format-conversion section 8, conversion of a format is performed in it, and file management is carried out to it at the filing Management Department 13.

[0025] Moreover, when alteration prevention mode is chosen, after MAC is added to a header by the approach described above with reference to drawing 2 , file management is carried out at the filing Management Department 13.

[0026] Moreover, when alteration detection mode is chosen, detection of the existence of the alteration to the image file which it was acquired from the external device through the storage 17 or the communication line 16 (PC, alteration test equipment, etc.), and was sent to the filing Management Department 13 is performed. That is, the image data to which MAC was added is divided into MAC and image data, image data is inputted into MD creation section 33 from the filing Management Department, and MAC is inputted into the decryption section 34. In MD creation section 33, MD is generated using predetermined functions, such as a Hash Function, from the inputted image data. Moreover, the decryption section 34 generates MD' using the public key Kpublic (camera) memorized by the public key memory 35. It judges whether the comparison coincidence section 32 compares MD and MD', and is in agreement. When both are not in agreement, it turns out that image data was altered by the 3rd person.

[0027] Moreover, secure mode is used when memorizing image data to a storage. In this case, image data is read from the filing Management Department 13, and it is inputted into the encryption section 36. The encryption section 36 enciphers this image data using the share key memorized by the share key memory 37, and sends the enciphered image data to the filing Management Department 13 again. Then, this enciphered image data demounts by control of the record-medium control section 15, and it is written in the possible storage 17.

[0028] Moreover, secure mode is used also when transmitting an image file through a communication line. In this case, image data is read from the filing Management

Department 13, and it is inputted into the encryption section 36. The encryption section 36 enciphers this image data using the share key memorized by the share key memory 37, and transmits the enciphered image data to external devices (PC, alteration test equipment, etc.) through a communication line 16 by control of the communications control section 14.

[0029] According to the above-mentioned 2nd operation gestalt, copyright can be kept by taking a photograph by normal mode, when photographing a snap image, and taking a photograph in digital-watermarking mode to alteration supervision mode and the image which wants to keep copyright, for example, in photoing the thing used as an image of evidence. Furthermore, preservation and transmission of data can be carried out to insurance by choosing secure mode to photo the high image of confidentiality and transmit an image file to insurance. Moreover, it becomes possible by combining two or more modes to use one camera for various applications from the above-mentioned effectiveness.

[0030] With reference to drawing 4 , the 3rd operation gestalt of this invention is explained below. In drawing 4 , the thing of the same reference figure as drawing 1 shall have the same function. Moreover, although the configuration in the communication facility of drawing 1 and the various modes of drawing 3 is omitted here, of course, you may have these functions. In the digital camera 103 of evidence which has the camera section 50-3, the image data obtained by picturizing a photographic subject with the image pick-up means 60 is memorized in an image memory 6. Image data is read from an image memory 6 to the file-format-conversion section 8, and it is changed into the graphics format of criteria, such as JPEG and TIFF. Thereby, the file format by which the data of header information were added to image data is created ((A) of drawing 5).

[0031] The information for personal authentication is read from IC card 40 for personal authentication with which the camera section 50-3 was equipped by control of the IC card control section 41 to coincidence, and it is inputted into the file-format-conversion section 8, and it is recorded as the information for personal authentication shows a header at (B) of drawing 5 . Next, in MD creation section 9, MD is created by applying predetermined functions, such as a Hash Function, to the whole data or image data, and the data for personal authentication ((C) of drawing 5). Next, in the MAC creation section 11, MAC is created by enciphering MD using the private key Kprivate (camera) memorized beforehand in the private key memory 10 ((D) of drawing 5). In addition to the data and the data for personal authentication of image header information, at the header Records Department 12, MAC is stored in an image header. Thereby, in a graphics format as shown in (E) of drawing 5 , an image file is saved at the filing Management Department 13, and file management is carried out.

[0032] Such an image file demounts by control of the storage control section 15, and in order to detect whether it was altered while being memorized and carried by the possible storage 17, alteration detection equipment 104 is used.

[0033] That is, the image file memorized by the storage 17 with which alteration test equipment 104 was equipped is read to the filing Management Department 19 by control of

the storage control section 18. At the filing Management Department 19, it separates into the whole data which need an image file to calculate MAC and the above mentioned MAC, i.e., the data except MAC, image data (header information other than the image data itself, such as JPEG and TIFF, may be included in this image data), and the data for personal authentication, MAC is inputted into the decryption section 21, and data required to calculate MAC are inputted into MD creation section 22. Furthermore, the data for personal authentication are inputted also into the individual humanity news read-out section 22.

[0034] In the decryption section 21, MD1 is generated by decrypting MAC using the public key Kpublic (camera) memorized beforehand in the public key memory 20. On the other hand, in MD creation section 22, MD2 is generated using predetermined functions, such as a Hash Function, from the inputted image data. Next, in the comparison coincidence section 23, when MD1 is compared with MD2 and both are not in agreement, it can judge with having been altered by the 3rd person.

[0035] Moreover, in the individual humanity news read-out section 42, specification of a photography person is performed by reading the data for personal authentication. Here, specification of a photography person is meaningful only when it is checked that image data is not altered.

[0036] According to the above-mentioned 3rd operation gestalt, not only the existence of an alteration of an image but an image photography person can specify by adding the information for personal authentication at the time of the data origination for alteration detection of image data. Especially, as information for a photography person's personal authentication, since the data for alteration detection are created from the data with which image data and the data for personal authentication were aligned using said encryption key, the alteration of image data and the alteration of a photography person's data for personal authentication are detectable with one alteration detection data here. If a photography person's data for personal authentication are not altered, a photography person can be specified from the data for personal authentication.

[0037] The 4th operation gestalt of this invention is explained below. In drawing 6 , the thing of the same reference figure as drawing 1 shall have the same function. Moreover, although the configuration in the communication facility of drawing 1 and the various modes of drawing 3 is omitted here, of course, you may have these functions. In the digital of-evidence camera system 105 which has the camera section 50-4, the image data obtained by picturizing a photographic subject with the image pick-up means 60 is memorized in an image memory 6. Image data is read from an image memory 6 to the file-format-conversion section 8, and it is changed into the graphics format of criteria, such as JPEG and TIFF. Thereby, the file format by which the data of header information were added to image data is created ((A) of drawing 7). Next, in MD creation section 9, MD1 or MD2 (B [of drawing 7 / (B)], (B)') is generated using predetermined functions, such as a Hash Function, from the whole data or image data. These MD1 and MD2 may be the same. MD1 is inputted into the MAC creation section 11. In the MAC creation section 11, MAC is

calculated using the private key Kprivate (camera) beforehand memorized by the private key memory 10, and MAC1 is created ((C) of drawing 7). This MAC1 is sent to the header Records Department 12.

[0038] On the other hand, MD2 is inputted into IC card 40' for personal authentication with which the camera section 50-4 was equipped through the IC card control section 41. In IC card40' for personal authentication, MD2 is enciphered using the private key Kprivate (IC card) memorized by internal private key memory, and MAC2 is created ((C)' of drawing 7). This MAC2 is sent to the header Records Department 12 through the IC card control section 41.

[0039] In addition to the data of image header information, at the header Records Department 12, MAC1 and MAC2 are stored in an image header. Thereby, in a graphics format as shown in (D) of drawing 7 , an image file is saved at the filing Management Department 13, and file management is carried out.

[0040] Such an image file demounts by control of the storage control section 15, and in order to detect whether it was altered while being memorized and carried by the possible storage 17, alteration detection equipment 106 is used.

[0041] That is, the image file memorized by the storage 17 with which alteration test equipment 106 was equipped is read to the filing Management Department 19 by control of the storage control section 18.

[0042] At the filing Management Department 19, an image file is divided into MAC1, MAC2, and image data (header information other than the image data itself, such as JPEG and TIFF, may be included in this image data), MAC1 is inputted into the decryption section 21-1, and image data is inputted into MD creation section 22-1. In the decryption section 21-1, MD1 is generated by decrypting MAC1 using the public key Kpublic (camera) beforehand memorized by public key memory 20'. A public key Kpublic (camera) and a private key Kprivate (camera) are keys which serve as a pair in encryption/decryption processing. On the other hand, in MD creation section 22-1, MD1' is generated using predetermined functions, such as a Hash Function, from the inputted image data. Next, in the comparison coincidence section 23-1, when MD1 is compared with MD1' and both are not in agreement, it can judge with being altered by the 3rd person.

[0043] Similarly, MAC2 is inputted into the decryption section 21-2, and image data is inputted into MD creation section 22-2. In the decryption section 21-2, MD2 is generated by decrypting MAC2 using the public key Kpublic (IC card) beforehand memorized by public key memory 20'. A public key Kpublic (IC card) and a private key Kprivate (IC card) are keys which serve as a pair in encryption/decryption processing.

[0044] On the other hand, in MD creation section 22-2, MD2' is generated using predetermined functions, such as a Hash Function, from the inputted image data. Next, in the comparison coincidence section 23-2, when MD2 is compared with MD2' and both are in agreement, a photography person can be specified.

[0045] According to the above-mentioned 4th operation gestalt, not only the existence of an alteration of an image but an image photography person can specify by adding the

information for personal authentication at the time of the data origination for alteration detection of image data. It is possible to apply especially, the electronic signature used with other information systems, such as an electronic mail and electronic commerce, as 2nd data for alteration detection, since the 2nd data for alteration detection created with the equipment of the camera exterior as information for a photography person's personal authentication here is used. Therefore, an infrastructure-[an electronic authentication office, electronic commerce, etc.] information system and the digital of-evidence camera system which was able to take cooperation can also be built.

[0046] Below, the 5th operation gestalt of this invention is explained. The 5th operation gestalt is related with the digital image edit system using the image server constituted from hardware, such as a board and a PCMCIA card. Here, in order to simplify explanation, the minimum configuration of an image server is assumed.

[0047] Conventionally, by the approach using the data for alteration detection used to document data, it was considered that it was altered when original data were changed, even when it was only small. However, about image data, processing of compression, a clipping, insertion of a caption, etc., etc. is needed on the property of data in many cases. If it is the case of the photograph using a film, only a required part can be burned on printing paper, or it is equivalent to describing a comment on the reverse side of a photograph. If there is a legal excuse, such processing will not be in charge of an alteration. There is the approach of what kind of processing was performed to original image data and recording the processing hysteresis as an approach for judging whether just processing was made.

[0048] With this operation gestalt, it detects whether it is altered with the hysteresis of the performed processing except the image server by using an image server in the image which processed the clipping of a field of compression of a part of image data, the addition of a caption, etc.

[0049] Drawing 8 consists of a personal computer 107-1 and an image server 107-2 which consists of a PCMCIA card with which this personal computer 107-1 can be equipped, as it is drawing showing the configuration of the image server system 107 of the 5th operation gestalt, for example, is shown in drawing 11 .

[0050] An operation of the 5th operation gestalt is explained with reference to the flow chart of drawing 9 below. First, the filing Management Department 72 acquires the image file of a format as shown in (A) of drawing 9 from a storage 70 by control of the storage control section 71. Or the image file concerned is acquired from an external device 93 by control of the communications control section 78 through a communication line 77 (step S1). In this case, an image file can be easily inputted from an external device by preparing the filing Management Department 72 connection terminals, such as a serial cable in which direct continuation is possible, and SCSI, IrDA. Moreover, the same effectiveness is acquired even when it has the terminal of network connections, such as Ethernet. Next, the MAC verification section 73 receives an image file from the filing Management Department 72, and verifies MAC1 (step S2). That is, the filing Management Department 72 divides an image file into MAC1 and image data, MAC1 is inputted into the decryption

section 75, and image data is inputted into MD creation section 76. The decryption section 75 is decrypted using the public key Kpublic (camera) memorized by the public key memory 74, and creates MD1. Moreover, MD creation section 76 creates MD1' using predetermined functions, such as a Hash Function. By comparing MD1 with MD1', the comparison coincidence section 79 sends the verification result about whether the image photoed with the camera is altered after that to the filing Management Department 72.

[0051] When not altered, an image file is inputted into the image editorial department 93 from the filing Management Department 72, and image edit by the user using the image edit tool 80 is performed (step S3). In this case, the contents of the image file are displayed on an image display device 82, looking at this screen, using data entry units (a keyboard, mouse, etc.) 84, various kinds of processings are required or a user 91 inputs data. 83 is the user interface of a user 91 and the image server 107. The hysteresis at the time of edit is recorded on the edit hysteresis Records Department 81. The edit hysteresis Records Department 81 reads the information for personal authentication from IC card 92 for personal authentication to coincidence by control of the IC card control section 85, and records on it into edit hysteresis. The above-mentioned edit is continued until directions of an edit halt are issued by the user and decision of step S5 serves as NO.

[0052] Since the image file after edit and the data of edit hysteresis are sent to the filing Management Department 72, the filing Management Department 72 records on an image header in a format as shows the information on edit hysteresis to (B) of drawing 9 (step S6). In leaving the information which specifies the photoed camera, it also records camera information on an image header in a format as shown in (C) of drawing 9 .

[0053] Next, the image file after edit and the data of edit hysteresis are inputted into MD creation section 87 of the renewal section 86 of an image file from the filing Management Department 72, and MD2 is created using predetermined functions, such as a Hash Function. Next, the MAC creation section 88 creates MAC2 by enciphering MD2 using the private key Kprivate of the image server 107 memorized beforehand (image server) in the private key memory 90 (step S7). At the header Records Department 89, it records on an image header in a format as shows this MAC2 by (D) of drawing 9 (step S8). In leaving the information which specifies a camera, it becomes a format as shown in (E) of drawing 9 . The image file to which MAC2 was added is sent to the filing Management Department 72, and after this, it demounts by control of the storage control section 71, and is saved at the possible storage 70, or this image file is sent to an external device 93 through a communication line 77 by control of the communications control section 78, and is saved.

[0054] Since it can check whether what kind of processing was performed from the original image file, or the contents of an image have been changed except an image server by using an image server according to the above-mentioned 5th operation gestalt, it is not altered even if it performs required processing on the property of a data compression or image data like field logging. Moreover, when creating the data for alteration detection added to an image file after edit by the image server, the user who edited the image can be specified by using the data for personal authentication.

[0055] Below, the 6th operation gestalt of this invention is explained. The 6th operation gestalt constitutes the image server in the 5th operation gestalt from software started on PC etc. Here, in order to simplify explanation, the minimum configuration of an image server is assumed.

[0056] Drawing 10 is drawing showing the configuration of the image server system 108 constituted by installing an image server in PC. Here, only a different point from the configuration of the 5th operation gestalt shown in drawing 8 is explained.

[0057] As the 6th operation gestalt shows to drawing 10 , it is [the MAC creation section 88 and] a private key Kprivate. The memorized private key memory 90 is formed in the interior of IC card 109 which can be detached and attached freely to the not the interior but image server 108 of the image server system 108. Moreover, the IC card control section 85 is formed in the interior of renewal section of image file 86' of the image server system 108.

[0058] The image file after edit and the data of edit hysteresis are inputted into MD creation section 87 of renewal section of image file 86', and MD2 is created using predetermined functions, such as a Hash Function. This MD2 is sent to the MAC creation section 88 of IC card 109 by control of the IC card control section 85. The MAC creation section 88 enciphers MD2 using a private key Kprivate (IC card), and creates MAC2. This MAC2 is recorded on an image header in a format as sent to the header Records Department 89 by control of the IC card control section 85 and shown in (D) of drawing 9 , or (E). In addition, the information for personal authentication is stored in IC card 109 like the 5th operation gestalt, and this is read and you may make it record into edit hysteresis.

[0059] Since according to the above-mentioned 6th operation gestalt in addition to the effectiveness of the 5th operation gestalt it constitutes from a storage in which attachment and detachment like an IC card of management of an encryption key and processing of encryption are free and other functions, such as edit of an image and creation of edit historical data, were constituted from software, it has the effectiveness that an image server can be built by low cost.

[0060] The 7th operation gestalt of this invention is explained below. The 7th operation gestalt consists of a public key server style and a public key acquisition / registration device of alteration test equipment and an image server about decryption key acquisition / registration system. For the private key as encryption and the public key as a decryption key which are used with this operation gestalt, as shown in drawing 13 (A), it is generated by the manufacturer according to the key generation device 120 at the time of manufacture of equipments, such as a digital camera 220, and the image server 221, IC card 222, among these a private key is built-in to equipment, It is registered. This private key is immediately eliminated by insurance and the positive approach after registration.

[0061] Moreover, a public key is memorized by the record medium 203 by the key registration section 202 of the public key server style 110 which equipment is made to correspond with the serial number as an identifier of a proper, and is shown in drawing 13 (B).

[0062] When performing alteration detection to alteration detection equipment and the

image by which public key acquisition / registration device 111 of an image server was photoed with the digital camera 220, the serial number of equipment is transmitted to the key retrieval section 204 through the communications control section 211, communication lines 210 and 209, and the communications control section 208 from the public key acquisition section 212. The key retrieval section 204 reads the public key corresponding to the serial number of equipment from a storage 203, and sends it to MD creation section 205. MD creation section 205 creates MD using predetermined functions, such as a Hash Function, and sends it to the MAC creation section 206. The MAC creation section 206 creates MAC using the private key beforehand memorized by the private key memory 207, and sends it to the public key acquisition section 212 through the communications control section 208, a communication line 209, a communication line 210, and the communications control section 211 with a public key. The public key acquisition section 212 sends the acquired public key and the serial number of equipment to the public key registration section 214. The public key registration section 214 registers a public key and the serial number of equipment concerned into the public key memory 213.

[0063] The data of a public key are sent to MD creation section 216 from the public key acquisition section 212, and MAC is sent to coincidence at the decryption section 217. MD creation section 216 creates MD from the data of this public key using predetermined functions, such as a Hash Function. The decryption section 217 creates MD' by decrypting MAC using the public key Kpublic of the key management server memorized by the public key memory 218 (key management server). The comparison coincidence section 215 detects an alteration by whether MD and MD' is compared and it is in agreement. It is the purpose that by which the camera obtained by means of communications and the public key of an image server were acquired from the just key management server, and that verification of MAC here checks whether it is further altered in the middle of the communication link.

[0064] In addition, you may make it send the public key registered into the public key server 110 to a user with safe means, such as mailing. According to the above-mentioned 7th operation gestalt, the decryption key of the data for alteration detection is acquirable by sending the serial number of equipment to a decryption key (public key) server. When it follows, for example, a decryption key server can be used from the Internet, the data for alteration detection can be acquired even from where among the world based on the serial number of a camera.

[0065] The 8th operation gestalt of this invention is explained below. The 8th operation gestalt is related with alteration prevention of a multiplex resolution image. When a document file changes a part, a text stops connecting, semantics will change and the contents will differ from the original file. Since redundancy of image data is high, even if it performs edit of some, such as modification of resolution, to it, a photographic subject can be recognized in many cases. Therefore, since being the magnitude beyond the need and wanting to drop resolution on the image size at the time of photography and an unnecessary part are reflected, in some cases, I want to start only a required part in the side using an image. However, the image server for alteration prevention must usually be

prepared, an image must be edited in the interior, and MAC must be added again.

[0066] So, in the 8th operation gestalt, in order to solve the above-mentioned problem, the image of an alteration prevention camera is saved in the format holding a multiplex resolution image. Drawing 1414 is drawing showing the configuration of the 8th operation gestalt of this invention. In the digital of-evidence camera section 112, the image data obtained by picturizing a photographic subject with the image pick-up means 60 is memorized in an image memory 6. Next, this image data is inputted into the image contraction section 300, and is changed into the image of two or more kinds of resolution. If the minimum resolution to which a user wants to guarantee an alteration through the MAC creation resolution directions section 302 is specified at this time, this will be sent to MD creation section 9 through the filing Management Department 13. In MD creation section 9, MD is created using predetermined functions, such as a Hash Function.

[0067] On the other hand, the private key created from the data of the camera proper memorized by the data memory 301 of a camera proper and the information for personal authentication read from IC card 40 for personal authentication by control of the IC card control section 41 is memorized by the private key memory 10. In the MAC creation section 11, MD created in MD creation section 9 using this private key is enciphered, MAC is created, and it sends to the filing Management Department 13. The filing Management Department 13 gathers the image data of two or more kinds of resolution in one file, adds MAC created from the data of resolution with which the above was specified further to the image data concerned, and saves by control of the storage control section 15 at a storage 17.

[0068] Drawing 16 is drawing for explaining the image data file of this operation gestalt. As shown in drawing 16 , the conversion to a low resolution from high resolution is specified beforehand. MAC is created from the data of the resolution which guarantees the alteration prevention directed in the MAC creation resolution directions section 302, and it records on the header or another MAC management file of image data.

[0069] On the other hand, in alteration test equipment 113, MAC and image data are read from a storage 17 by control of the storage control section 18, and it sends to the filing Management Department 19. At the filing Management Department 9, MAC is sent to the decryption section 21 and image data is sent to an image memory 303. In the decryption section 21, MD1 is created by decrypting MAC using a public key. Moreover, after the image data memorized in the image memory 303 is reduced by the contraction approach predetermined in the image contraction section 304, it is sent to MD creation section 22, and MD2 is created using predetermined functions, such as a Hash Function. In the coincidence comparator 23, it judges whether image data was altered by comparing MD1 with MD2.

[0070] With reference to drawing 15 , the 9th operation gestalt of this invention is explained below. The 9th operation gestalt holds the image of multiplex resolution, and the image of each resolution has the intention of preventing the alteration of the graphics format in which the small block of fixed size is stored as a unit. The reason for storing the small block as a unit in this graphics format is because some images can be referred to at a

high speed.

[0071] Although the operation of the digital camera 114 of evidence is the same as an operation of the above-mentioned digital camera 112 of evidence, while having image contraction / division section 305 and creating the image of two or more resolution here, as shown in drawing 17 , with this operation gestalt, an image is divided per Brock of fixed magnitude. At the filing Management Department 13, MAC is created for every smallness Brock and MAC is written in the header for every small block. The image file with MAC is memorized by the storage 17 as an original image by control of the record-medium control section 15.

[0072] The user whose whole photographic coverage and resolution of an image are unnecessary creates logging of a required part and the image of required resolution from the original image read from the storage 17 within common PC115 using the edit software 306 at the time of photography. A user inputs into the image editorial department 306 by making the location of a required image part, size, resolution, etc. into the edit parameter 307. At the filing Management Department 13, the corresponding image block of a location is extracted from the corresponding image of resolution, and it saves at another image file.

[0073] When inspecting an alteration with alteration detection equipment 116, an edited image is read from a storage 17 to the filing Management Department 19 by control of the storage control section 18. In the alteration detection section 308, alteration detection is performed to an edited image. If MAC added for every small block from the first is added to a file new as it is at this time, even if it will not prepare an alteration prevention image server, a user can perform an editing task called modification of field logging of an image or resolution, giving proof nature to an image. Moreover, if it adds the data which recorded the procedure of filtering, without changing the pixel value itself in performing filtering, such as contrast stretching and smoothing, the guarantee of an original image will be attained also about a filtering image.

[0074] In addition, invention of the following configurations is included in the above-mentioned concrete operation gestalt.

1. Image Pick-up Section for being Digital of-Evidence Camera System Which Detects Alteration of Image Data Which Picturized Photographic Subject with Camera and was Obtained, and Picturizing Photographic Subject, The cipher-processing section which creates the data for alteration detection from the image data obtained by the image pick-up using the encryption key built in beforehand, the camera to provide and the alteration detection section which detects whether said data for alteration detection were decrypted using the decryption key corresponding to said encryption key, and said image data was altered based on the result of this decryption -- since -- the digital of-evidence camera system characterized by becoming.

(The operation effectiveness) According to this invention, it can check whether image data is altered by creating the data for alteration detection using the encryption key in a camera from image data, and decrypting this data for alteration detection using the decryption key corresponding to said encryption key. The weight of the evidence of the digital image it was

presupposed that it was inferior of a digital image by this compared with the image conventionally photoed using the film can be heightened.

[0075] Moreover, by this invention, although the encryption key for creating the data for alteration detection is not revealed outside by any means including a camera user, since the encryption key for creating the data for alteration detection is beforehand stored in the camera, it can manage an encryption key on very [in hard] high security level.

2. Said cipher-processing section is the digital of-evidence camera system of the configuration 1 publication characterized by creating said data for alteration detection by enciphering the data obtained by said image data with the application of the predetermined function using said encryption key.

(The operation effectiveness) At least, for change, extent of the alteration to image data is a predetermined function (for example, Hash Function) so that it may appear greatly. Since the data for alteration detection were created by enciphering to the data applied and obtained, the data for alteration detection which can ensure alteration detection can be offered.

3. Said alteration detection section is the digital of-evidence camera system of the configuration 2 publication characterized by detecting whether said image data was altered by comparing the data obtained by said image data with the application of said predetermined function with the data which decrypted said data for alteration detection using said decode key, and were obtained.

(The operation effectiveness) Since said data for alteration detection are used, alteration detection can be ensured.

4. Said cipher-processing section is the digital of-evidence camera system of the configuration 1 publication characterized by creating said data for alteration detection based on said encryption key and the data for personal authentication.

(The operation effectiveness) Not only the existence of an alteration of an image but an image photography person can specify by adding the information for personal authentication at the time of the data origination for alteration detection of image data.

5. Said cipher-processing section is the digital of-evidence camera system of the configuration 4 publication characterized by creating the 1st data for alteration detection using said encryption key, creating the 2nd data for alteration detection using said data for personal authentication, setting said 1st and 2nd data for alteration detection from said image data, and considering as said data for alteration detection from said image data.

(The operation effectiveness) Since it uses as data for alteration detection in accordance with the 1st data for alteration detection created from image data, and the 2nd data for alteration detection created from a photography person's data for personal authentication It is possible to apply said 2nd data for alteration detection like the electronic signature used with other information systems, such as an electronic mail and electronic commerce. An infrastructure-[an electronic authentication office, electronic commerce, etc.] information system and the digital of-evidence camera system which was able to take cooperation can also be built.

6. Digital of-evidence camera system of configuration 4 publication characterized by having had the storage section which memorizes said data for personal authentication, and said encryption key, and the 2nd cipher-processing section which creates the 2nd data for alteration detection from said data for personal authentication, and constituting said this 2nd cipher-processing section free [attachment and detachment] to said camera.
(the operation effectiveness) they be the media (IC card etc.) which can be detach and attach freely to a camera about the 2nd cipher processing section which memorize the data for personal authentication , and an encryption key , and create the 2nd data for alteration detection . by having prepare , even when carrying this medium and the camera of others who do not use usually be use , the existence of an alteration of the image which the individual attested and photoed certainly can be check .
7. Said cipher-processing section is the digital of-evidence camera system of the configuration 4 publication characterized by creating said data for alteration detection using said encryption key from the data with which said image data and said data for personal authentication were aligned.
(The operation effectiveness) In the case of the approach of creating the data for alteration detection using said encryption key, as information for a photography person's personal authentication, the alteration of image data and the alteration of a photography person's data for personal authentication are detectable with one alteration detection data from the data with which image data and the data for personal authentication were aligned. If a photography person's data for personal authentication are not altered, a photography person can be specified from the data for personal authentication.
8. Image Pick-up Section for being Digital of-Evidence Camera System Which Detects Alteration of Image Data Which Picturized Photographic Subject with Camera and was Obtained, and Picturizing Photographic Subject, The cipher-processing section which creates the data for alteration detection from the image data obtained by the image pick-up using the encryption key built in beforehand, The camera to provide and the alteration detection section which detects whether said data for alteration detection were decrypted using the decryption key corresponding to said encryption key, and said image data was altered based on the result of this decryption, since -- the alteration supervision mode as which, as for said camera, said image data detects whether it was altered or not -- in addition, with the secure mode in which encryption to the image data transmitted to said alteration detection section from said camera is performed It has the digital-watermarking mode which embeds digital-watermarking data at image data, and the normal mode which performs the usual photography without using a security function. The digital of-evidence camera system characterized by having the mode selection section for choosing the mode of at least one request from these modes.
(The operation effectiveness) By equipping a camera with the optional feature in various modes, the function of the request according to the purpose of using a camera can be set up. For example, when photographing a snap image, taking a photograph by normal mode and photoing the thing used as an image of evidence, copyright can be kept by taking a

photograph in digital-watermarking mode to alteration supervision mode and the image which wants to keep copyright. Furthermore, preservation and transmission of data can be carried out to insurance by choosing secure mode to photo the high image of confidentiality and transmit an image file to insurance. Moreover, it becomes possible by combining two or more modes to use one camera for various applications from the above-mentioned effectiveness.

9. Decryption Key Storage Section Memorized in accordance with 1st Decryption Key corresponding to 1st Encryption Key Generated by Equipment corresponding to Identifier of Proper, and this Identifier, The decryption key output section which creates the data for alteration detection about said 1st decryption key using the 2nd encryption key, and is outputted in accordance with this data for alteration detection, and said 1st decryption key, A preparation ********** server and the decryption key storage section which memorizes said 1st decryption key acquired from said decryption key server through means of communications etc., Said data for alteration detection supplied from said decryption key server through means of communications etc. are decrypted using the 2nd decryption key corresponding to said 2nd encryption key. the decryption key acquisition section equipped with the alteration detection section which detects whether said 1st decryption key was altered based on the result of this decryption -- since -- decryption key acquisition - characterized by becoming Registration system.

(The operation effectiveness) According to this invention, the decryption key of the data for alteration detection is acquirable by sending the serial number of equipment to a decryption key server. When it follows, for example, a decryption key server can be used from the Internet, the data for alteration detection can be acquired even from where among the world based on the serial number of a camera.

10. With Filing Management Department Which is Digital Image Edit System into which Image Data is Edited, and Does Filing Management of the Image Data Inputted through Image Input Section while Detecting Alteration of Image Data While decrypting the 1st data for alteration detection beforehand given to said image data using the decryption key corresponding to the encryption key used when creating this data for alteration detection The alteration detection section which detects the alteration condition of image data by comparing this the 1st decoded data for alteration detection and said image data, To said image data from the edited image data to which various image processings were performed by the image editorial department which performs various kinds of image processings, and said image editorial department, and the data of the edit hysteresis by said image editorial department the renewal section of an image file which creates the 2nd data for alteration detection using an encryption key other than said encryption key, and adds this to said edited image data -- since -- the digital image edit system characterized by becoming.

(The operation effectiveness) According to this invention, since the data for alteration detection are created in accordance with image data and edit hysteresis, it can check what kind of edit processing has been performed to the original image, and can detect further whether image edit processing is performed except the system concerned.

11. Said renewal section of an image file is the digital image edit system of the configuration 10 publication characterized by using said another encryption key for said personal authentication information, and creating said 2nd data for alteration detection while being able to detach and attach freely to a digital image edit system and memorizing said personal authentication information and said another encryption key.
(The operation effectiveness) An image server can be built by low cost with constituting other functions, such as edit of an image and creation of edit historical data, from a storage in which attachment and detachment like an IC card of management of an encryption key and processing of encryption are free by software.
12. The digital image edit system of the configuration 9 publication characterized by uniting and recording personal authentication information on said edit hysteresis.
(The operation effectiveness) The person who edited the image can be specified by including the information for personal authentication in image data also including the data of image edit hysteresis.
13. Said image input section is the digital image edit system of the configuration 9 publication characterized by inputting the image data memorized by external storage by connecting with said image filing section through direct continuation (a cable, IrDA) or a communication line.
(The operation effectiveness) An image file can be easily inputted from an external device by equipping the image filing section of an image server with the terminal of direct continuation, such as a serial cable, and SCSI, IrDA, and the terminal of network connections, such as Ethernet.
14. It is a digital of-evidence camera system the configuration 1 characterized by for said image data be multiplex resolution image data which made the group two or more image data different mutually [resolution] , and memorized it , and said cipher-processing section have the selection section which chooses at least one image data which has desired resolution out of said multiplex resolution image data in order to create said data for alteration detection , or given in ten .
(The operation effectiveness) By specifying the resolution which guarantees alteration detection at the time of record, the user using an image becomes possible [using a desired resolution image without being dependent on the resolution at the time of photography].
15. it be a digital of evidence camera system the configuration 1 which said image data be a multiplex resolution image data which made the group two or more image data different mutually [resolution] , and memorized them , and each image data in said multiplex resolution image data be memorize considering the predetermined small block as a unit , and said cipher processing section be said small block unit , and be characterize by create said data for alteration detection , or given in ten .
(The operation effectiveness) Alteration detection can be carried out also to the image which performed image edit like a clipping, without preparing the server of dedication by adding alteration detection data for every small block.
[0076]

[Effect of the Invention] According to this invention, the weight of the evidence of a digital image can be heightened, the digital of-evidence camera system and decryption key acquisition / registration system which can manage an encryption key on very high security level can be offered, and even if it edits further compression which is needed on the property of an image, field logging, insertion of a caption, etc., the digital image edit system which can maintain the weight of the evidence of a digital image can be offered.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is drawing showing the digital of-evidence camera structure of a system concerning the 1st operation gestalt of this invention.

[Drawing 2] It is drawing showing a procedure until MAC is added to image data.

[Drawing 3] It is drawing showing the configuration of the digital camera of evidence concerning the 2nd operation gestalt of this invention.

[Drawing 4] It is drawing showing the digital of-evidence camera structure of a system concerning the 3rd operation gestalt of this invention.

[Drawing 5] It is drawing showing a procedure until the data for personal authentication and MAC are added to image data.

[Drawing 6] It is drawing showing the digital of-evidence camera structure of a system concerning the 4th operation gestalt of this invention.

[Drawing 7] It is drawing showing a procedure until MAC1 and MAC2 are added to image data.

[Drawing 8] It is drawing showing the image server structure of a system concerning the 5th operation gestalt of this invention.

[Drawing 9] It is a flow chart for explaining an operation of the 5th operation gestalt.

[Drawing 10] It is drawing showing the image server structure of a system concerning the 6th operation gestalt of this invention.

[Drawing 11] It is drawing showing the example of the image server structure of a system of the 5th operation gestalt.

[Drawing 12] It is drawing showing the example of the image server structure of a system of the 6th operation gestalt.

[Drawing 13] It is drawing showing decryption key acquisition / registration structure of a system concerning the 7th operation gestalt of this invention.

[Drawing 14] It is drawing showing the digital of-evidence camera structure of a system concerning the 8th operation gestalt of this invention.

[Drawing 15] It is drawing showing the digital of-evidence camera structure of a system concerning the 9th operation gestalt of this invention.

[Drawing 16] It is drawing for explaining the image data file concerning the 8th operation gestalt.

[Drawing 17] It is drawing for explaining the image data file concerning the 9th operation

gestalt.

[Description of Notations]

1 -- Image pick-up lens,
2 -- Image sensor,
3 -- Amplifier,
4 -- A/D-conversion section,
5 -- Signal-processing section,
6 -- Image memory
7 -- Image display section,
8 -- File-format-conversion section,
9 -- MD creation section,
10 -- Private key memory,
11 -- MAC creation section,
12 -- Header Records Department,
13 -- Filing Management Department,
14 -- Communications control section,
15 -- Storage control section,
16 -- Communication line,
17 -- Storage,
18 -- Storage control section,
19 -- Filing Management Department,
20 -- Public key memory,
21 -- Decryption section,
22 -- MD creation section,
23 -- Comparison coincidence section,
24 -- Communications control section,
25 -- Communication line,
50-1 -- Camera section,
60 -- Image pick-up means,
100 -- Digital camera of evidence,
101 -- Alteration test equipment.